Developing the Network Centric Functional Concept, as Well as Associated Concepts, Architectures, and Studies

The network centric functional concept identifies capabilities, attributes, measures and metrics associated with the transformation to a fully netted force. The purpose of the concept is to:

- Provide the measurement framework for evaluating joint initiatives and conducting analyses in support of the Joint Capabilities Integration and Development System (JCIDS; CJCSI 3170.01D).
- Generate thought and discussion about new methods for performing Joint Functions (Force Application, Protection, C2, Battlespace Awareness, Focused Logistics, Network Centric, etc.) across the range of military operations.
- Provide the conceptual framework for developing integrated architectures used for analyzing joint capabilities.
- Provide the basis for military experiments and exercises.

The network centric functional concept is intended for the JFC at the operational level of war in the 2015 timeframe. Assumptions, capabilities, attributes and metrics are the essence of concept development. While the concept will serve as a key enabler of the network centric environment – the technical domain, it will extend beyond the technical domain by identifying net centric functional warfighting capabilities across the full range of military operations within the human and technical elements.

Improving Training and Education

Recent operational Joint Task Force (JTF) lessons learned, major combat operations lessons learned, and reports from wargames and exercises indicate that future combat operations will be fought with Joint Forces led by joint headquarters that effectively combine the expertise and capabilities of each of the Services. The “task-organized” nature of forming a JTF headquarters in parallel with force

threats and vulnerabilities inherent in a networked force. Ultimately, every user of the network will have a role in its defense.

deployment of Service and functional component headquarters requires well-trained personnel in joint C4 operations.

While each of the Services has a robust capability to train C4 personnel in their specialties, these programs are focused at the company grade officer and junior enlisted level for the purpose of entry-level proficiency training. Despite the fact that our information systems constitute a key enabler to network centric operations, the DOD has inadequate technical training programs. Continuous joint training, and not just entry/mid-grade level joint training is required to effectively plan, engineer, manage and defend the complex C4 architectures supporting Joint Force operations today. The improvement of education and training of joint C4 professionals will be accomplished by:

- Influencing the Direction of the Major "Learning Areas" (CJCSI 1800.01) as defined for our existing Joint Professional Military Education (JPME) Programs (e.g. Intermediate Level Course, Senior Level Course, JPME Phase II and 1-star CAPSTONE) and evolving JPME programs (e.g. JPME 101, Joint Advanced Warfighting School (JAWS), Senior Enlisted JPME and 3-star CAPSTONE). At a minimum, this community of "users" must be familiar with the capabilities enabled by a network centric environment as well as the potential

- Defining Core Competencies and Training Standards for Joint Force Personnel qualified in Joint C4 Planning, Management and Information Assurance Operations. To ensure joint C4 training addresses the requirements of the Joint Force, core competencies and training standards must be defined.

- Creating a Joint C4 Planners Course to better support Joint Operations. As military staffs prepare for the major joint operations of today and the complex network centric operations of tomorrow, one thing remains consistent: C4 networks will continue to be a key enabler for battlefield successes. The Joint C4 Planners Course is aimed at field grade officers, senior warrant officers and senior enlisted personnel. The intent of the course is to use joint planning processes and tools to train students in the art and science of joint C4 planning, installation and operation.

- Developing computer based training (CBT) packages for distance learning (DL). The development of CBT/DL packages will support both prerequisite requirements and follow-on training to the Joint C4 Planners Course.

- Assessing and Evaluating Joint Information Assurance (IA)/Computer Network Defense (CND) Training. A thorough review of current policies and training courses regarding certification

of network administrators and IA specialists is required. This must include the effectiveness of the mechanisms employed to enforce these standards. As our networks become more and more critical, sufficient resources must be committed to training those responsible to employ, protect, monitor, defend and recover the network from potential attacks.

- Supporting a "Fight As You Train" Network Centric Environment. The environment must allow commanders to conduct modeling, simulation, wargaming, exercises and rehearsals using the same systems and interfaces that the Joint Force will employ in actual operations.

Providing the "Right Network Management and Modeling and Simulation Tools to Do the Job"

Not counting sensors and weapon platforms, DOD has over three million computers – most of which reside on some network. To ensure networks are reliable and secure, C4 personnel must have comprehensive, yet simple to use tools that allow them to plan, operate, manage, reconfigure and secure the network in battlefield conditions.

- Fielding Information Assurance Tools. To effectively protect the GIG, the joint C4 community needs to follow industry's lead of simplifying network security challenges by using standardized configuration management. Personnel responsible for IA and CND require standardized tools that defend the whole GIG, provide rapid intrusion detection and monitoring and facilitate timely, automatic software security updates. USSTRATCOM has the lead in advocating the capabilities and tools required to defend the GIG through implementation of an enterprise-wide solution. Combatant Commanders, Services and Agencies must make IA and CND a priority in the budget process and work to implement USSTRATCOM-identified capabilities.

- Developing GIG NetOps and Joint Network Management Tools with Global C4 Situational Awareness. Paramount to successful network centric operations is the ability to manage the GIG from the strategic to the tactical level. As IP-based networked systems such as JTRS are fielded, the joint C4 community must ensure that support tools are fielded. GIG NetOps requires an integrated approach that accounts for Service-unique CONOPS and network configurations. One tool should be capable of providing the management services required for the whole network, including the critical capability for the network to self-form and self-heal to fill gaps created during the course of military operations. Network management must be simplified and designed for joint C4 staffs at senior headquarters down to the Soldiers, Marines, Airmen, and Sailors forward deployed under hostile fire. Bottom line: A "simpler is better" approach is needed.

The network management "tool box" must account for IP management as well as the efficient use and management of the frequency spectrum. These tools should provide real-time access to information on IP and frequency spectrum information to

determine available resources. Network centric operations of the future require the ability to dynamically and automatically reconfigure and move. As with IA, an enterprise solution is what is required to fully integrate and operate in a joint environment.

- Implementing Standard Communications and Computing Modeling and Simulation (M&S) Tools for War Planning. C4 M&S enables joint network planners and managers to predicatively analyze the performance and sufficiency of planned networks and proposed network changes. It enables C4 planners to analyze and understand network traffic loading under the stresses of full combat operations, as well as assessing and understanding the impacts of new systems and applications on networks.

JC2 will contain a M&S tool compatible with and integrated into existing operational warfighting simulation tools in order to ensure coordination and coherence between operations and communications and computing planning. This tool will interface to the GIG network management facility to rapidly effect changes in configurations in order to accommodate current warfighting operations. Joint C4 planners and managers will incorporate the powerful potential of modern M&S technologies into their planning and management processes.

Network Simulation

- Ensuring Critical Infrastructure Protection (CIP). An effective network centric environment requires the assured availability of a robust C4 infrastructure. Assuring the availability and security of such an infrastructure requires pro-active and dynamic action by both DOD and industry.

  □ Required joint community actions:

  — Fully understand what C4 assets (physical and logical) are critical to mission accomplishment and fully understand their interdependencies.

  — Develop and apply standard criteria to assess the vulnerabilities of and associated threats to the C4 infrastructure.

  — Apply an aggressive risk-management methodology to develop and implement courses of action to avoid or mitigate risks to the C4 infrastructure and, if needed, effectively respond to and reconstitute following events that negatively impact infrastructure capabilities.

  — Develop cooperative working relationships with the telecommunications industry to ensure the actions listed above are

completed for C4 infrastructure assets not under DOD control but central to mission accomplishment.

— Determine the feasibility of incorporating the monitoring of Supervisory Control and Data Acquisition (SCADA) systems supporting C4 CIP locations into DOD network management plans.

☐ Required industry actions. Since non-DOD entities provide a significant and growing percentage of the GIG infrastructure, Industry needs to:

— Identify the critical nodes and single points of failure for the infrastructure they provide.

— Develop a plan for physical facility decentralization for critical infrastructures. As telecommunications facilities are modernized, there is a growing trend to consolidate services within facilities. Industry must weigh the impacts of a potential attack on the telecommunications infrastructure with consolidation efforts.

— Have computerized facility records that allow the tracking of physical routes used for information flow.

— Conduct periodic audits of those records to ensure facility diversity is maintained.

■ Enhancing Information Management. The joint C4 community must forge the path necessary to better handle management of critical information to ensure Joint Forces are able to maintain decision superiority. Information management is in an early development phase. As DOD expands capabilities in this area with better tools and techniques and incorporates content staging in NCES, the joint C4 community will enable better information management. The tools must support the delivery of the right information, to the right person, at the right time, in the right format, using the most efficient means available.

Improving Joint Configuration Management Procedures

As a community, great lengths were taken to define the specific technical configuration for employment of joint communications systems. The CJCSM 6231 series identifies the standards by which C4 capabilities are provided to Joint Forces. However, Joint Forces continue to experience issues when C4 units from different Services are brought together in support of contingency operations. Today, C4 professionals are expected to be able to integrate legacy C4 systems with state-of-the-art commercial and military capabilities. Since high-quality C4 services are required, common standards must be developed and enforced for the employment of C4 systems, and consistency must be maintained throughout the platform/application lifecycle.

■ Establishing Joint Network Configuration Management Standards. In an era of global sourcing of forces to meet contingencies and operations, the joint community needs to institutionalize C4 employment standards. Ad hoc network configurations between Combatant

Commanders, Services and multinational forces will not support the employment of robust, reliable networks. Take, for example, the different standards for the employment of multiplexer technology. Based upon the region a unit is tasked to support, C4 planners must be prepared to employ IDNX/Promina, FCC-100 or CODEM multiplexers to support the Joint Forces operating in that region. The byproduct of this lack of standardization is an increase in training, supply and maintenance requirements.

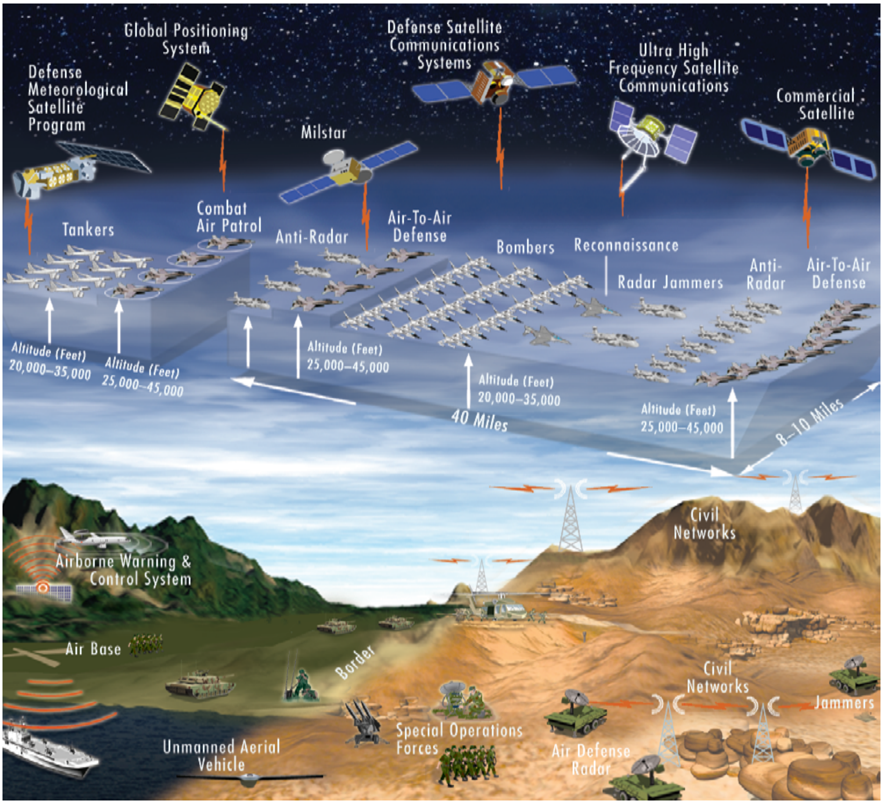
> ″If we did configuration management on our ships and aircraft like we do on our networks…our ships wouldn't sail and aircraft wouldn't fly.″
>
> — *LtGen R. M. Shea,*
> *Director for C4 Systems,*
> *The Joint Staff*

As C4 units deploy to a joint operations area, C4 planners must be able to expect a common set of capabilities between like units. Often times, post-fielding upgrades to systems allows for the provisioning of enhanced capabilities to warfighting forces. While the C4 community must continue to strive to meet the needs of commanders, a balanced approach must also be pursued in order to retain consistency in the capabilities provided to Joint Forces.

- Improving Lifecycle Management. Historically, C4 professionals have achieved mission accomplishment through workarounds (the C4–equivalent of duct tape and bailing wire) to integrate and connect a multitude of systems. A greater disciplined approach to lifecycle management is required. The burden is not just on those individuals involved in implementing and managing networks, it also impacts software developers. Maintaining and fielding multiple versions of application software, C2 systems and operating systems is difficult, expands training requirements and increases the chance of system incompatibility where interoperability was once achieved. For example, basic software applications, like those used in the office environment, require configuration management across DOD to ensure functionality is maximized and units are not forced to operate at the lowest common denominator in terms of capabilities. Extend this to C2 systems and the ultimate price of poor lifecycle management could be lives lost in combat.

Ensuring Spectrum Availability

No resource is misunderstood more than the frequency spectrum. This limited resource is used by all Services; federal, state and local agencies; and other nations. As technology expands and more wireless capabilities are fielded, competition for spectrum usage will likewise increase.


Global Positioning System
Defense Meteorological Satellite Program
Defense Satellite Communications Systems
Ultra High Frequency Satellite Communications
Commercial Satellite
Milstar
Tankers
Combat Air Patrol
Anti-Radar
Air-To-Air Defense
Bombers
Reconnaissance
Radar Jammers
Anti-Radar
Air-To-Air Defense
Altitude (Feet) 20,000–35,000
Altitude (Feet) 25,000–45,000
Altitude (Feet) 25,000–45,000
Altitude (Feet) 20,000–35,000
40 Miles
Altitude (Feet) 25,000–45,000
8–10 Miles
Civil Networks
Airborne Warning & Control System
Air Base
Border
Civil Networks
Jammers
Unmanned Aerial Vehicle
Special Operations Forces
Air Defense Radar

DOD Spectrum Use

■ Developing a Frequency Spectrum Strategy. To better manage this commodity, the joint C4 community requires a comprehensive frequency spectrum strategy that maximizes spectrum availability and takes into account fielding of future systems. The strategy must also address how to:

□ Ensure worldwide DOD access to frequency spectrum to include de-conflicting with host nation civil use of military spectrum, negotiating tariffs and legal rights. Because spectrum allocation, allotment, and assignment varies from region-to-region and country-to-country, Combatant Commanders must continue to work with host nation counterparts to ensure this world resource in a public domain is available for training and contingency use. Since there is no guarantee that a foreign government will allow DOD use of required spectrum to support operational needs, Combatant Commanders need to identify spectrum concerns and issues respective to their area of responsibility.

□ Ensure system developers are educated on international frequency restrictions and that systems account for these restrictions and potential impact on training in both the normal operating environment and in peacetime.

- □ Take into account industry plans for spectrum use.

- Reallocating Frequency Spectrum. Numerous federal and DOD bands are candidates for future reallocation. Frequency bands below 3 GHz have unique attributes attractive for commercial applications. The potential consequences of reallocation are significant. The joint community must continue to be fully engaged to ensure that spectrum remains available and unimpeded for critical system use. Further reallocation must address national security, full-cost reimbursement and the availability of "comparable" spectrum. DOD personnel also need a better understanding of Industry's investment direction.

- Evaluating Frequency Spectrum Managers Training. Professional spectrum managers are the backbone to successful network operations. As GIG transformational systems such as JTRS come on line, and DOD achieves the tenet of "every battlespace entity is a potential node", effective management of spectrum is paramount. New concepts such as Wideband Network Waveform, all-in-one spectrum management tools, and the vastly increased potential for frequency interference due to proximity of so many emitters requires advanced training. Adequacy of current frequency spectrum training courses and personnel must be assessed and modified accordingly to meet 21st century GIG requirements.

- Educating Both the C4 Community and Users. CONUS spectrum moves affect multiple platform acquisition programs and deployed equipment usage. What appears as a logical spectrum design decision in CONUS may have enormous impacts when systems are deployed OCONUS. Careful study and analysis must be done prior to any agreement to move a system to an alternative band.

Implementing the DOD Network Centric Data Strategy

The core of the network centric environment is the data that enables effective decisions. In this context, data implies all data assets such as system files, databases, documents, official electronic records, images, audio files, web sites, and data access services. One DOD goal, as confirmed by the Deputy Secretary of Defense in Management Initiative Decision 905, is to populate the network with all data (intelligence, non-intelligence, raw, and processed) and change the paradigm from "process, exploit, and disseminate" to "post before processing." All data is advertised and available for users and applications when and where they need it. To support this DOD goal and a network centric environment of shared data, Services and Agencies must:

- Register their metadata elements in the DOD Metadata Registry.

- Develop catalogs/databases of metadata information (based on established standards).

- Build systems to the Service Oriented Architecture using agreed upon interoperability profiles.

- Make sure steps are taken to affiliate every system to one or more community of interest (COI) and that the COIs have worked to harmonize their data exchange requirements.

- Ensure that COIs begin the process of creating taxonomy (hierarchical classification of data) and ontology (annotations of data relationships) within their domain.

Deputy Secretary of Defense

Paul Wolfowitz

February 2004

“We have to take ‘Jointness’ to a new and higher level. Technology permits it. The organization needs to get out of the way of it.”